ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

МУҲАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ

АХБОРОТ-КОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИНИНГ РИВОЖЛАНИШ ИСТИҚБОЛЛАРИ

мавзусидаги

Республика илмий-амалий анжуман
МАЪРУЗАЛАР ТЎПЛАМИ

(20-21 апрель)

ҚАРШИ-2018

appliance. This redirection requires that a biometric authentication is provided before buffered content is saved to the PVR. Thus, the recording process is actuated by providing fingerprint data to the local client which transfers the authentication data to the main server. To simplify our implementation content is buffered and encrypted on the rebroadcast server and redirected to the PVR appliance where it is saved directly to the hard disk.

C. Enrollment Toolset

Biometric data for enrollment can be input at the server-side, but it is more practical to enable enrollment from client-side appliances. There are slight risks that biometric data could be intercepted during the initial enrollment process, but in order to achieve widespread adoption of this type of content protection system we consider that ease-of-use should take priority. Thus we consider that local devices may be regarded as "trusted". Note that a secure mechanism for sharing private keys between appliances was described in [1] and requires that a user provide an identical biometric token at both appliances within a certain timeout period.

Two principle types of biometric data are used – active inputs and passive, or observational inputs. The active inputs, fingerprint data in our case, are entered from a laptop using a simple computer application and a fingerprint scanner. A user must provide 3-4 good quality fingerprints and the system will confirm enrollment. There is also a test function to verify that a user's fingerprint is correctly recognized by the system after enrollment. A similar application is used for face enrollment and requires that a standard USB webcam is connected to the laptop. We have found that HMM based face recognition is most reliable achieving reliable enrollment from a short video clip if the user simply nods their head slowly from left to right.

D. Observational Authentication

This mode was initially added to the system as an experiment. It provides an interesting alternative to single-event authentication and represents a new approach to controlling access to content. When observational authentication mode is activated the system scans a field of view in the vicinity of the living room viewing area and performs regular face detection on this viewing area. Detected face regions are compared against enrolled faces and as long as at least one of the people viewing the content is authorized the system continues to decode the media stream. If no authorized user is found the system enters a timeout mode and after a few minutes will flash a warning to the viewers. After a second timeout period it will flash a second warning and content decryption will cease about a minute later. When faces are detected but none of these correspond to an authenticated user the system can either cease decoding the media stream, or alternatively can provide a reduced quality rendering of the content. When an authenticated user returns to the viewing area, or an authenticated fingerprint is input then normal viewing can be resumed.

IV. Conclusions

Our overall conclusion is that biometric techniques are becoming sufficiently reliable and mature to warrant further exploration of their use in CE applications. There are still many problems to be solved but the potential to address fundamental issues such as access control to digital content is quite compelling.

References

[1] P. Corcoran & A. Cucos, Techniques for securing multimedia content in consumer electronic appliances using biometric signatures, IEEE Transactions on Consumer Electronics, Vol. 51, No. 2, May 2005, pp. 545-551

NETWORK TRAFFIC CLASSIFICATION AND MANAGEMENT METHODS

Teshaboev Khujamiyor Normatjon ogli, TUIT named after Muhammad Al-Khwarizmi,
Department of H and SMST, Second course of master,

Traffic management is a difficult problem because it fundamentally involves a balance between conflicting objectives: statistical sharing versus isolation. At one extreme, statistical sharing of network resources without reservations is desirable to achieve a high efficiency. But

since demand can exhaust resources, it is difficult (if not impossible) to guarantee QoS without reservations. At the other extreme, it is well known that QoS can be guaranteed by reserving resources for each traffic flow. Reservations isolate resources for each traffic flow so that flows do not have to compete for resources.

Another general principle is that traffic controls can be exercised simultaneously at various levels. At the node level, routers and switches are responsible for packet scheduling and selective packet discarding. Ingress nodes can perform access policing. Nodes may be capable of explicit congestion notification. At the network level, the network makes admission control decisions to accept or block new packet flows. At the higher level, transport or application layer protocols can be adaptive to the congestion level in the network[1].

Traffic control methods can be classified as preventive or reactive. Reactive methods are activated to ameliorate congestion after it is detected. For example, TCP reacts to congestion by reducing TCP source rates. A general principle is that prevention of congestion is preferred to reacting to congestion. If congestion occurs, packets will be lost, and it takes time to clear the queues in congested nodes. Preventive methods such as explicit congestion notification are preferred because congestion and packet loss may be avoided.

In practice, networks generally depend on a variety of traffic controls employed at different points in the networks. The main preventive traffic control is admission control. Admission control gives the network an opportunity to make a decision whether to accept or reject a new traffic flow before the flow begins. Admission control can be quite effective in protecting the network from congestion by blocking new traffic flows at the network ingress. Typically, admission control relies on a signaling protocol that allows applications to explicitly request a QoS or service class. Information about the new traffic flow (e.g., peak rate, average rate, burstiness) must be provided to the network at the same time so that sufficient resources can be allocated. A signaling protocol is not absolutely necessary if the required QoS can be inferred implicitly from knowledge about the traffic. For example, the telephone network uses admission control. Since every telephone call requires the same QoS, the required QoS does not have to be signaled explicitly[4].

Access or ingress policing is another preventive traffic control that typically accompanies admission control. Since admission control decisions are based on information about the accepted new traffic, it is important that source traffic conforms to the given parameters because excessive traffic could degrade network performance to the point of violating QoS guarantees. The most widely used algorithm for access policing is the leaky bucket. The leaky bucket algorithm is simple to implement with counters, and allows adjustable tolerance for bursty traffic sources. For conforming traffic, the access policing should be invisible and make no difference. For excess traffic, three actions are possible: the excess traffic is admitted; admitted but marked with lower priority; or discarded immediately.

Packet scheduling is an essential traffic control because it recognizes that packets have different forwarding requirements. Packet scheduling should recognize different service priorities and give preferential treatment to packets with more stringent delay requirements. Buffer management is a complementary problem to packet scheduling. Whereas packet scheduling deals with the order of packets to depart from a buffer, buffer management dictates how incoming packets should fill up limited buffer space.

Buffer management should recognize different loss priorities and selectively discard packets of lower loss priority. In a way, loss priorities may be viewed as priorities related to space, while service priorities are related to time. In addition to simple loss priorities, packets may be discarded in coordination with higher layer protocols. For example, random early detection (RED) is a random packet discarding strategy that takes advantage of the congestion control algorithm in TCP to improve network throughput and stability.

Instead of simply discarding packets during congestion, it is better to avoid congestion entirely if possible. Congestion might be avoided by inferring the state of congestion in the network by watching for long packet delays and packet losses. This does not require the network to provide any congestion information. However, the most effective way to avoid congestion is explicit congestion notification by the network. Traffic sources are given enough advance warning to slow

down and prevent congestion. This so-called closed loop control works only for some adaptable applications that can adjust their transmission rate dynamically.

Admission Control. Admission control is one of the most effective means of congestion control. The objective is to prevent congestion by blocking new packet flows before the flow begins. If a new flow is accepted, the network is explicitly or implicitly agreeing to provide the required QoS for the duration of the flow. This agreement is explicit if the admission control is carried out with a signaling protocol[1].

Many approaches to admission control can be found in the literature. As shown in Figure 1, Figure 2 and Figure 3, approaches can be classified according to where the acceptance decision is made: hop-by-hop, endpoint or edge router, or centralized bandwidth broker (BB). Hop-by-hop admission control follows the traditional approach of telecommunications networks. A signaling message requesting resources attempts to find a path through the network. Each router or switch along the path has an opportunity to accept and forward the request, or reject and block the request. Although this is a natural approach, the complexity required for routers limits the scalability to large networks.

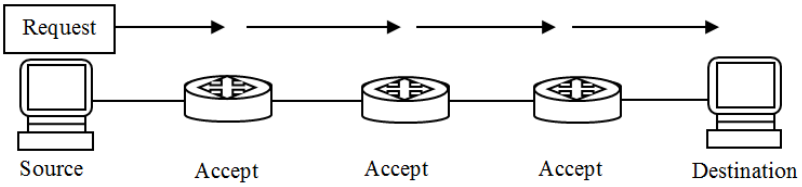

Figure 1. Hop-by-hop admission.

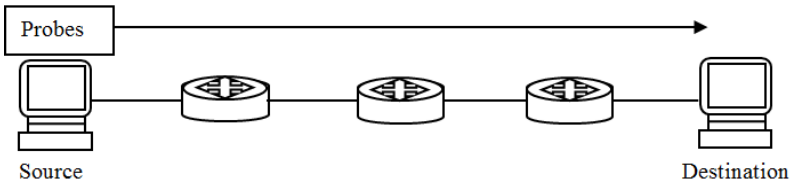

Figure 2. Endpoint admission.

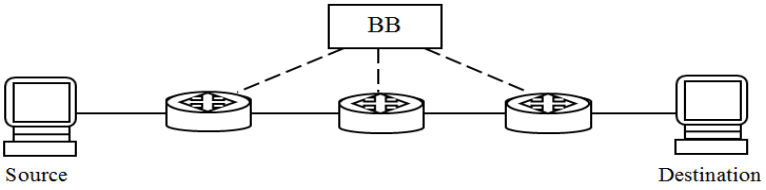

Figure 3. Centralized bandwidth broker.

The second approach leaves the admission decision to the source endpoint (host) or an edge (ingress or egress) router. The decision can be based on data collected passively (without any extra effort) or actively by special probe packets. This approach simplifies the role of the core network, resulting in better scalability.

The third approach is also aimed at better scalability. Admission into each network domain is controlled by a centralized bandwidth broker. The available resources of the domain are monitored by the bandwidth broker, which makes all admission decisions and keeps track of accepted traffic flows[6]. The bandwidth broker concept has two potential advantages. It keeps the core network stateless for scalability. Also, it can make network-wide optimal resource allocation decisions.

In order to make an acceptance or rejection decision, the network must estimate the amount of bandwidth and buffer resources needed for a new traffic flow. The required resources are compared with the available resources. The network also estimates the hypothetical impact of the new traffic flow on the current network performance. There must be assurance that the new flow will not cause the QoS for current traffic flows to fall below acceptable levels.

Approaches for admission control can be alternatively classified by how the decision is made: deterministic, stochastic, or measurement-based. Deterministic approaches use worst-case bounds. In contrast, stochastic approaches assume statistical characteristics of the traffic for more accurate

estimation of required resources. However, the accuracy of stochastic approaches depends heavily on the choice of traffic models. Traffic modeling is a difficult problem due to the dynamic nature of network traffic. Measurement-based approaches attempt to avoid the modeling problem by using measurements of the actual traffic instead of assumed traffic models.

Access control. Access control or policing refers to regulation of ingress traffic at the user-network interface. There are reasons for regulating traffic at the network edge and not internally within the network. At the network boundary, excessive traffic can be blocked before consuming any network resources. Moreover, it is natural to verify conformance of the traffic as close to the source as possible before the traffic shape is effected by other packet flows. Finally, individual packet flows at the network edge are slower than multiplexed flows in the core network[3].

Traffic contracts. When an admission control decision is made, that decision is based on traffic descriptors and QoS parameters provided by traffic sources. If the network admits a packet flow, it might be said that the user and network have agreed upon a traffic contract. Unlike SLAs, traffic contracts are a misnomer because they are not legal agreements. A traffic contract is an implicit understanding between the network and sources that both sides are cooperating in admission control. Sources are obligated to conform to the traffic descriptors that they provided for the admission decision. Excessive traffic will consume more network resources and deteriorate the QoS seen by all users. In accepting a new flow, the network is obligated to provide and sustain the requested QoS.

Traffic classification. Packets must be classified to determine their QoS requirements. In the IntServ framework, reservations are made for individual flows. Packets belonging to the same flow can be identified by these IP header fields: source IP address, destination IP address, source port number, destination port number, and protocol.

Packet classification is difficult due to at least two reasons. First, routers must process terabytes of packets per second. Thus, packet classification must be done very quickly and efficiently. Second, there may be an enormous number of flows going through a router. Classification of a packet to a particular flow essentially involves a table search, but the table could be enormous. Packet classification is an ongoing research problem that is central to router design.

In the Diffserv framework, packets must be classified at the ingress to the Diffserv network such that an appropriate Diffserv codepoint (DSCP) can be assigned. The DSCP is encoded in the first six bits of the Type of Service (ToS) field in the IPv4 packet header. The DSCP identifies the per hop behavior (PHB) to be applied to the packet.

Traffic regulation. The rate of traffic entering the network can be regulated as a means of enforcing the traffic contract. Since admission control decisions are based on traffic parameters given for a packet flow, it is important that flows do not exceed their stated parameters because excessive traffic would deteriorate the network performance seen by all users[4].

The goal of traffic regulation is to differentiate between conforming and non-conforming packets (according to the traffic contract). Conforming packets should be allowed immediate entrance into the network as if the traffic policer was transparent. Non-conforming packets may be discarded immediately or allowed entrance with some kind of packet marking. The former is preferred if the network load is heavy, then it would be better to discard the non-conforming packets to avoid any wasted use of network resources. The idea behind packet marking is that the purpose of the network is to carry packets. If the network load is light, it does no harm to carry non-conforming traffic. If congestion is encountered anywhere, the marked packets can be discarded first.

In the Diffserv framework, packets may also be classified into flows which are subject to policing and marking according to a traffic conditioning agreement (TCA). The TCA includes traffic characteristics (such as token bucket parameters) and performance metrics (delay, throughput) as actions required for dropping out of profile packets. Out of profile packets are non-conforming packets, and either dropped or marked with a lower priority level.

Traffic shaping. Traffic shaping can be done at the source prior to entrance into the network or within the network. Traffic shaping at the source is a means of self regulation in order to ensure

conformance to the traffic contract. Conformance is desirable to minimize the amount of traffic discarded at the network ingress.

Traffic shaping within the network is not concerned with a traffic contract. The idea is that smooth traffic will cause smaller queues and hence incur shorter queueing delays and less delay jitter. Since traffic shaping is done by buffering, some queueing delay is added by the traffic shaper, but then smooth traffic should flow more quickly along the rest of the path. Overall, network performance is improved by keep traffic smooth.

Traffic shaping refers to the practice of providing different treatments to different classes of traffic. Each individual packet that arrives is examined and classified (mostly based on DPI). According to the priority of each class of traffic, packets are put into queues and then transmitted. This allows an ISP to give priority to certain classes of traffic, leaving whatever bandwidth is left over for others[4].

NGN АРХИТЕКТУРАСИДА ДАСТУРЛИ КОММУТАТОР - SOFTSWITCH ВА МАРШРУТИЗАТОРЛАР ИМКОНИЯТЛАРИ

Б.С.Назаров, “Ўзбектелеком” АК Қашқадарё филиали Бешкент телекоммуникация боғламаси муҳандиси, ТАТУ Қарши филиали катта ўқитувчиси,
С.А. Норкобилов, ТАТУ Қарши филиали ассистенти
М.М.Келдиёров, ТАТУ Қарши филиали талабаси

NGN (Next generation Network) кейинги авлод алоқа тармоғи яратилади. Бунда нутқ, видео, аудио, графика ва ҳоказо узатиш мумкин. Ахборот пакетли шаклда узатилади. NGN архитектурасининг асосий элементлари асосийси дастурли коммутатор - Softswitch ҳисобланади.

Softswitch – чақирувларни назорат қилиш, сигнализация, протоколларнинг ўзаро ишлашини, конвергент тармоқ ичида хизматлар яратилишини амалга оширадиган стандарт дастурий модулларнинг ўзаро ишлаш модулидир. International Packet Communication Consortion (IPCC, олдинги International Softswitch Consortiun) Softswitch технологиясининг тўртта: алоқа агенти, сигнализация шлюзи, иловалар сервери ва охирги ускуналарни бошқариш таянч компонентини ишлаб чиқди.

Алоқа агенти (Session agent). Сигнализация шлюзи (Singnaling gateway) амалдаги 7-сон УКС УФТф тармоғининг амалдаги сигнализацияси билан интеграцияси учун ва Softswitch негизидаги тармоқда Интеллектуал Тармоқ (IN) имкониятларини қувватлаш учун қурилма ҳисобланади.

Иловалар сервери (Application servers) Softswitch технологиясига IP технологияси негизидаги унификацияланган почтани, конференцияларни таъминлаш ва IP centrex хизматларини кўрсатиб, айрим кўп қирраликни қўшади. Ушбу серверлар SIP протоколи ёки бошқа протоколлар ёрдамида Softswitch чақирувларни назорат қилиш элементлари билан ўзаро ишлайди.

Ўзаро ҳисоб-китобни бошқариш сервери (Back-end servers) ҳисобларни юритиш, авторизациялаш ва солиқ солиш, биллингни қувватлаш ва шу каби функцияларни амалга оширади. Асосий имкониятлар чақирувларни детализация қилиш, ўзаро ҳисоблар ва IP-телефониянинг иловаларини Web-браузеридан бошқариш марказининг провайдери каби ташкил этувчиларнинг ўз вазифалари бўйича қарама-қарши функцияси ҳисобланади. Улар IP тармоқларда «crank bank» каби маълум бўлган вақтинчалик бузилган ҳолатларда УФТф тармоғига чақирувлар қайта адресланади.

Ушбу компонентлар тармоқларнинг эксклюзив ишланма ҳисобланган УФТф маҳсулотлар каналларини коммутация қилиш учун негиз саналганлигидан фарқли равишда очиқ стандартлар билан замонавий дастурий таъминотга асосланган чақирувлар учун коммутация ва назорат қилиш тузилмасига бирлаштирилган. Ускуна етказиб берувчилар Softswitch тузилмасини унинг таркибига турли компонентларни, эҳтиёжлар ва конструкцияга боғлиқ ҳолда, киритилишини ўзгартириши мумкин. Имкониятларни кенгайтириш учун